REMARKS/ARGUMENTS

Claims 1-48 are pending. Claims 1-25 have been withdrawn from consideration. Claims 26-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hawes (USPN 5,070,528) in view of Hagerman (USPN 6,973,568).

Hawes states "In accordance with one of the protocols described in this specification, encryption is performed at a transmitting or source node and decryption is performed at a destination node. This is known as end-to-end encryption, as contrasted with link encryption, in which decryption and re-encryption are performed at each intermediate node between the source and the destination. The manner in which encryption is performed, or the encryption algorithm, is of no particular consequence to the present invention. Nor is it of any consequence whether encryption and decryption keys are exchanged in advance between the sending and receiving nodes, or whether a public key system is used for the establishment of keys. As will be noted later in this description, one implementation of the invention uses an encryption algorithm known as the Data Encryption Standard (DES), as defined by FIPS-46 (Federal Information Processing Standard-46) published by the National Institute of Standards and Technology (formerly the National Bureau of Standards). However, the invention is not limited to this, or any other encryption algorithm." (Hawes: column 8, lines 6-23)

"The identification of every conceivable packet format would be complex and time-consuming. Moreover, the present invention is not limited to parsing logic capable of identifying particular packet formats. By way of example, several types of formats are identified in the receive data path of a presently preferred embodiment of the invention. These formats are shown diagrammatically in FIGS. 9a-9b, 10 and 11. FIGS. 9a-9b show two variants of the packet format known as SNAP/SAP, including a Data Link encryption format defined by Digital Equipment Corporation (FIG. 9a), and the DOD-IP encryption format (FIG. 9b). FIG. 10 shows the ISO end-to-end encryption packet format, and FIG. 11 shows a third format, known as SILS, which is still in the process of being defined in the industry." (Hawes: column 10, lines 45-60)

Hagerman states "The key value used to compute the authentication code field 300 is extracted from a key table 170, 172, 174, 176, 178, and 180 associated with each port. These key tables may be, and often are, dissimilar from port to port, for example key table 170 need not be the same as key table 172. The key tables are initialized such that the key table associated with a

given port contains keys for communication with the ports that the given port is authorized to communicate with. For example, if port 130 is authorized to communicate through port 138 and storage system 110 to logical unit 114, key table 170 associated with port 130 and key table 178 associated with port 138 will have at least one common key for port 138--port 130 communications. If port 132 is not authorized to communicate with port 138, then key table 172 and key table 178 will not have a common key for port 132--port 138 communications." (Figure 3 Description)

The material cited by the Examiner does not teach or suggest any security enable indicator. The material cited describes various encryption formats, but does not teach or suggest any first frame having a security enable indicator and a second frame having a security control indicator. Furthermore, it is respectfully submitted that none of the materials teach or suggest including any security enable indicator in the first frame where the first frame is associated with a fabric login or port login message.

Nonetheless, to facilitate prosecution, the independent claims have been amended to variably recite "wherein the security enable parameter is used by the first network entity when the first network entity is added to the fibre channel network to determine if the second network entity supports security." This amendment is believed supported by the original Claims, Specificaiton, and Drawings. For example, "According to various embodiments, the techniques of the present invention embed a security enable parameter in an authentication message. When a new network entity is introduced into a fibre channel fabric, the new network entity transmits an initialization message with the security enable parameter. The receiving network entity may or may not support security. If the receiving network entity supports authentication, the receiving network entity can extract the security enable parameter and transmit a response acknowledging authentication capabilities. Other information can be exchanged during an authentication sequence to provide for future security in transmissions between the two network entities. In one example, the two entities can exchange cryptographic material in the authentication sequence to allow common key generation." (page 11, lines 21-31)

The materials cited by the Examiner do not teach or suggest any security enable parameter used when the first network entity is added to the fibre channel network to determine if the second network entity supports security. The Examiner argues that Hawes describes a cryptographic preamble "that includes an offset field to indicate the location of data to be

cryptoraphically processed as well as a mode field indicating the type of cryptographic processing to be performed." It is acknowledged that Hawes describes a cryptographic preamble. The Examiner appears to argue that the cryptographic preamble can be both the security enable indicator in a first frame and the security control indicator in a second frame. It is respectfully submitted that even if the cryptographic preamble is interpreted as a security enable indicator and a security control indicator, there is no cryptographic preamble sent to determine whether the receiving network entity supports security when the source entity is added to the fibre channel network.

Furthermore, the independent claims have been amended to variably recite "receiving an acknowledgment from the second network entity indicating that the second network entity supports security, the acknowledgement including key and algorithm information and a salt parameter." This amendment is supported by the original Claims, Specification, and Drawings. For example, "If the network entity 403 supports security, the network entity 403 identifies the security enable parameter and transmits an acknowledgement at 415 to network entity 401 indicating support for security. According to various embodiments, the transmission at 415 includes a salt parameter." (page 12, lines 9-12)

The materials cited by the Examiner do not teach or suggest any security enable parameter message that is acknowledged with algorithm information and a salt parameter. The message with a "cryptographic preamble" in Hawes is not acknowledged with algorithm information and a salt parameter.

Furthermore, it is respectfully submitted that none of the materials teach or suggest including any security enable indicator in the first frame where the first frame is associated with "a fabric login (FLOGI) or port login (PLOGI) message" as now recited in the independent claims. Transmitting a cryptographic preamble in a fabric login or port login message to a node that does not support security may cause deleterious effects. Hagerman is not believed to teach or suggest using any login, fabric login, port login, or FLOGI and PLOGI messages to include a security enable indicator. Hawes does not use any fabric login or port login messages because Hawes describes a packet network system that does not have any fabric login or port login mechanisms.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
Weaver Austin Villeneuve & Sampson LLP

/Audrey Kwan/

G. Audrey Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100